Claims

1. Telecommunication network with a first domain (PLMN-A) comprising at least one mobile application part protocol instance connected to a gateway node (MSEGA) which is adapted to send and receive mobile application part messages and which is connectable to a second domain (PLMN-B, PLMN-C),
characterised in that the gateway node (MSEGA) is adapted to receive a mobile application part message from the first domain (PLMN-A), to convert the received mobile application part message obtaining a secured mobile application part message, and to send the obtained message towards the second domain (PLMN-B, PLMN-C), the gateway node (MSEGA) further being adapted to receive a secured mobile application part message from the second domain (PLMN-B, PLMN-C), to extract an unsecured mobile application part message from the received secured mobile application part message and to send the extracted message towards the first domain (PLMN-A).

2. Telecommunication network according to any of the preceding claims, wherein the gateway node (MSEGA) is connectable to a third domain (PLMN-E) and wherein the gateway node (MSEGA) performs a selective discarding of mobile application part messages received from the first domain (PLMN-A) and destined for the third domain (PLMN-E) and a selective discarding of mobile application part messages received from the third domain (PLMN-E) and destined for the first domain (PLMN-A).

3. Telecommunication network according to claim 3, wherein the gateway node (MSEGA) performs as a firewall towards the third domain (PLMN-E).

4. Telecommunication network according to any of the preceding claims wherein the gateway node (MSEGA) is connectable to different domains, and levels of security are configurable for the different domains.

5. Telecommunication network according to claim 5 wherein for a particular domain a fallback to a lower level of security than the configured level of security for the particular domain is allowable and wherein the allowing of the fallback to the lower level of security is configurable for one domain independently from a configuring of an allowing of a respective fallback to a lower level of security level for another domain.

6. Gateway node (MSEGA) comprising an interface (NI) to a first domain (PLMN-A) of a telecommunication network for sending and receiving mobile application part messages,
characterized in that the gateway node (MSEGA) comprises an interface (ZFI) to a second domain (PLMN-B, PLMN-C) of the telecommunication network for sending and receiving secured mobile application part messages and that the gateway node (MSEGA) comprises a conversion unit (CU) that is adapted to receive a mobile application part message via the interface (NI) to the first domain (PLMN-A), to convert the received mobile application part message obtaining a secured mobile application part message, and to send the obtained message via the interface towards the second domain, the conversion unit further being adapted to receive a secured mobile

application part message via the interface (ZFI) to the second domain (PLMN-B, PLMN-C), to extract an unsecured mobile application part message from the received secured mobile application part message and to send the extracted message via the interface (NI) towards the first domain (PLMN-A).

7. Gateway node (MSEGA) according to claim 7, comprising an interface to a third domain (PLMN-E) for sending and receiving mobile application part messages and a filtering unit adapted to perform a selective discarding of mobile application part messages.

8. Gateway node (MSEGA) according to claim 8, wherein the gateway node (MSEGA) performs as a firewall towards the third domain (PLMN-E).

9. Gateway node (MSEGA) according to any of the claims 7 to 9, wherein the gateway node (MSEGA) is connectable to different domains, and the gateway node (MSEGA) comprises a security database (SPD) for storing indications of levels of security for the different domains.

10. Gateway node (MSEGA) according to claim 10, comprising a fallback store (FBS) for storing for a particular domain an indication that a fallback to a lower level of security than the configured level of security for the particular domain is allowable and wherein the allowing of the fallback to the lower level of security is configurable for one domain independently from an allowing of a respective fallback to a lower level of security for another domain.